



NOMBRE DE ALUMNO: VICTOR
HUGO LÓPEZ MORENO

NOMBRE DEL PROFESOR (A):
ANDRÉS ALEJANDRO REYES
MOLINA

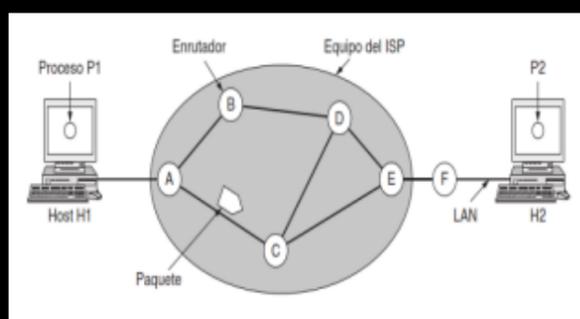
NOMBRE DEL TRABAJO:
SUPERNOTA

MATERIA: REDES DE
COMPUTADORAS II

GRADO: 6°

3.1. CONMUTACIÓN DE PAQUETES DE ALMACENAMIENTO Y REENVÍO

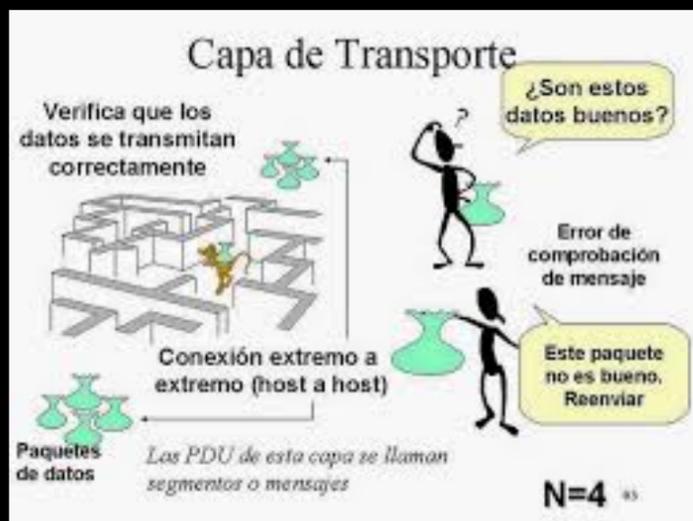
Antes de empezar a explicar los detalles sobre la capa de red, vale la pena volver a exponer el contexto en el que operan los protocolos de esta capa. En la figura 5-1 podemos ver este con texto. Los componentes principales de la red son el equipo del Proveedor del Servicio de Internet (ISP) (enrutadores conectados mediante líneas de transmisión), que se muestra dentro del óvalo sombreado, y el equipo de los clientes, que se muestra fuera del óvalo. El host H1 está conectado de manera directa a un enrutador del ISP, A, tal vez en forma de una computadora en el hogar conectada a un módem DSL.



En contraste, H2 se encuentra en una LAN (que podría ser una Ethernet de oficina) con un enrutador, F, el cual es propiedad del cliente, quien lo maneja. Este enrutador tiene una línea alquilada que va al equipo del ISP. Mostramos a F fuera del óvalo porque no pertenece al ISP. Sin embargo y para los fines de este capítulo, los enrutadores locales de los clientes se consideran parte de la red del ISP debido a que ejecutan los mismos algoritmos que los enrutadores del ISP (y nuestro principal interés aquí son los algoritmos)

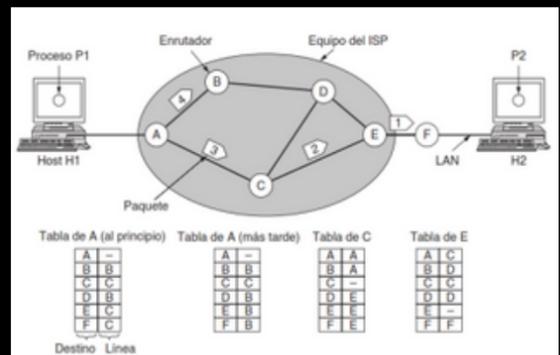
3.2. SERVICIOS PROPORCIONADOS A LA CAPA DE TRANSPORTE

La capa de red proporciona servicios a la capa de transporte en la interfaz entre la capa de red y de transporte. Una pregunta importante es qué tipo de servicios proporciona precisamente la capa de red a la capa de transporte. Hay que diseñar los servicios de manera cuidadosa, con los siguientes objetivos en mente: 1. Los servicios deben ser independientes de la tecnología del enrutador. 2. La capa de transporte debe estar aislada de la cantidad, tipo y topología de los enrutadores presentes. 3. Las direcciones de red disponibles para la capa de transporte deben usar un plan de numeración uniforme, incluso a través de redes LAN y WAN. Un bando (representado por la comunidad de Internet) declara que la tarea de los enrutadores es mover paquetes de un lado a otro, y nada más. Desde su punto de vista (basado en casi 40 años de experiencia con una red de computadoras real), la red es de naturaleza no confiable, sin importar su diseño. Por lo tanto, los hosts deben aceptar este hecho y efectuar ellos mismos el control de errores (es decir, detección y corrección de errores) y el control de flujo.



3.3. IMPLEMENTACIÓN DEL SERVICIO SIN CONEXIÓN

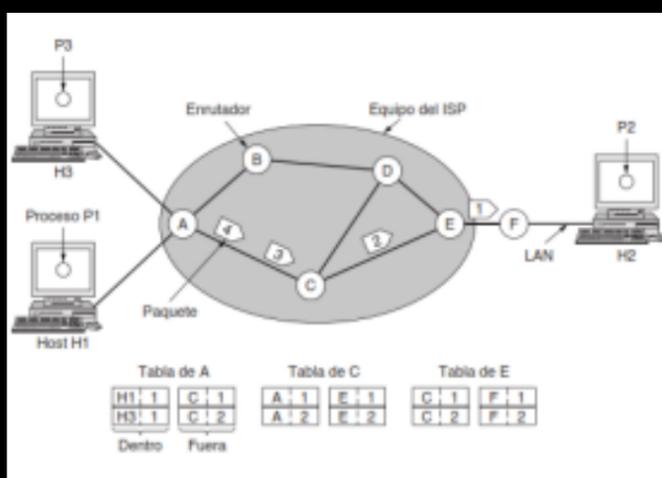
Puesto que ya vimos las dos clases de servicios que la capa de red puede proporcionar a sus usuarios, es tiempo de analizar el funcionamiento interno de esta capa. Se pueden realizar dos formas de organización distintas, dependiendo del tipo de servicio ofrecido. Si se ofrece el servicio sin conexión, los paquetes se transmiten por separado en la red y se enrutan de manera independiente. No se necesita una configuración por adelantado. Ahora veamos cómo funciona una red de datagramas. Suponga que el proceso P1 de la figura 5-2 tiene un mensaje largo para P2. Dicho proceso entrega el mensaje a la capa de transporte y le indica a ésta que lo envíe al proceso P2 en el host H2. El código de la capa de transporte se ejecuta en H1, por lo general dentro del sistema operativo. Dicho código agrega un encabezado de transporte al frente del mensaje y entrega el resultado a la capa de red, que quizá sólo sea otro procedimiento dentro del sistema operativo.



Supongamos para este ejemplo que el mensaje es cuatro veces más largo que el tamaño máximo de paquete, por lo que la capa de red tiene que dividirlo en cuatro paquetes: 1, 2, 3 y 4; y enviar cada uno por turnos al enrutador A mediante algún protocolo punto a punto; por ejemplo, PPP. En este momento entra en acción el ISP. Cada enrutador tiene una tabla interna que le indica a dónde enviar paquetes para cada uno de los posibles destinos. Cada entrada en la tabla es un par que consiste en un destino y la línea de salida que se utilizará para ese destino. S

3.4. IMPLEMENTACIÓN DEL SERVICIO ORIENTADO A CONEXIÓN

Para el servicio orientado a conexión necesitamos una red de circuitos virtuales. Veamos ahora cómo funciona. La idea detrás de los circuitos virtuales es evitar la necesidad de elegir una nueva ruta para cada paquete enviado, como en la figura. Cuando se establece una conexión, se elige una ruta de la máquina de origen a la máquina de destino como parte de la configuración de conexión y se almacena en tablas dentro de los enrutadores. Esa ruta se utiliza para todo el tráfico que fluye a través de la conexión, de la misma forma en que funciona el sistema telefónico. Como ejemplo, considere la situación que se muestra en la figura 5-3. En ésta, el host H1 ha establecido una conexión 1 con el host H2. Esta conexión se recuerda como la primera entrada en cada una de las tablas de enrutamiento. La primera línea de la tabla A indica que si un paquete con el identificador de conexión 1 viene de H1, se enviará al enrutador C y se le dará el identificador de conexión 1. De manera similar, la primera entrada en C enruta el paquete a E, también con el identificador de conexión 1.



3.5. COMPARACIÓN ENTRE LAS REDES DE CIRCUITOS VIRTUALES Y LAS REDES DE DATAGRAMA

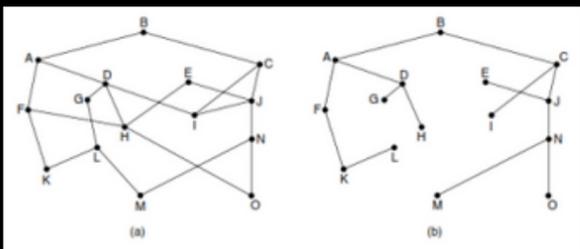
Tanto los circuitos virtuales como los datagramas tienen sus seguidores y sus detractores. Ahora intentaremos resumir los argumentos de ambos bandos. Los aspectos principales se listan en la figura, aunque es probable que los puristas puedan encontrar ejemplos contrarios para todo lo indicado en la figura:

Dentro de la red existen ventajas y desventajas entre los circuitos virtuales y los datagramas. Una de ellas tiene que ver con el tiempo de configuración y el tiempo de análisis de la dirección. El uso de circuitos virtuales requiere una fase de configuración que necesita tiempo y recursos. Sin embargo, una vez que se paga este precio, es fácil averiguar qué hacer con un paquete de datos en una red de circuitos virtuales: el enrutador sólo usa el número de circuito para buscar en una tabla y encontrar hacia dónde va el paquete. En una red de datagramas no se requiere configuración, pero se requiere un procedimiento más complicado para localizar la entrada correspondiente al destino. Un aspecto relacionado es que las direcciones de destino que se utilizan en las redes de datagramas son más largas que los números de los circuitos que se utilizan en las redes de circuitos virtuales, ya que tienen un significado global. Si los paquetes tienden a ser bastante cortos, incluir una dirección de destino completa en cada paquete puede representar una cantidad considerable de sobrecarga y, por ende, un desperdicio de ancho de banda

Aspecto	Red de datagramas	Red de circuitos virtuales
Configuración del circuito.	No necesaria.	Requerida.
Direccionamiento.	Cada paquete contiene la dirección de origen y de destino completas.	Cada paquete contiene un número de CV corto.
Información de estado.	Los enrutadores no contienen información de estado sobre las conexiones.	Cada CV requiere espacio de tabla del enrutador por cada conexión.
Enrutamiento.	Cada paquete se enruta de manera independiente.	La ruta se elige cuando se establece el CV; todos los paquetes siguen esa ruta.
Efecto de falias del enrutador.	Ninguno, excepto para paquetes perdidos durante una caída.	Terminan todos los CVs que pasaron por el enrutador defectuoso.
Calidad del servicio.	Difícil.	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV.
Control de congestión.	Difícil.	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV.

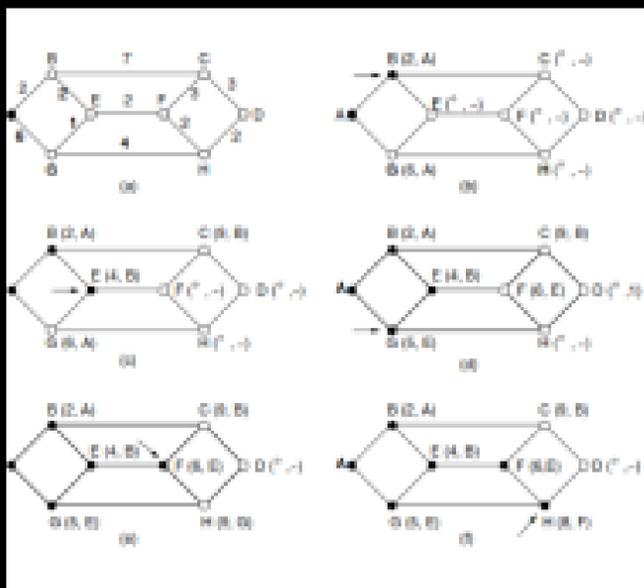
3.6. PRINCIPIO DE OPTIMIZACIÓN

Antes de entrar en algoritmos específicos, puede ser útil señalar que es posible hacer un postulado general sobre las rutas óptimas sin importar la topología o el tráfico de la red. Este postulado se conoce como principio de optimización (Bellman, 1957) y establece que si el enrutador J está en la ruta óptima del enrutador I al enrutador K, entonces la ruta óptima de J a K también está en la misma ruta. Para ver esto, llamemos r_1 a la parte de la ruta de I a J y r_2 al resto de la ruta. Si existiera una ruta mejor que $r_1 r_2$ entre J y K, se podría concatenar con r_1 para mejorar la ruta de I a K, lo cual contradice nuestro postulado de que $r_1 r_2$ es óptima. Como consecuencia directa del principio de optimización, podemos ver que el grupo de rutas óptimas de todos los orígenes a un destino dado forman un árbol con raíz en el destino. Dicho árbol se conoce como árbol sumidero (o árbol divergente) y se ilustra en la figura, donde la métrica de distancia es el número de saltos. El objetivo de todos los algoritmos de enrutamiento es descubrir y usar los árboles sumidero para todos los enrutadores.



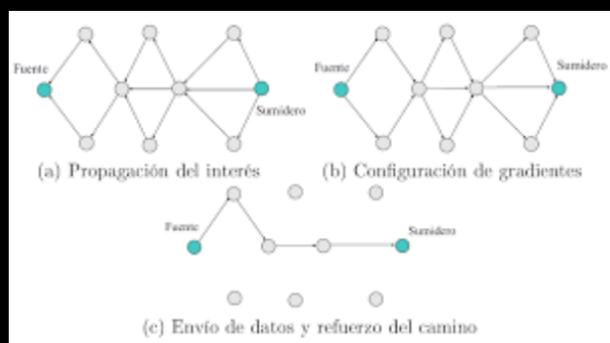
3.7. ALGORITMO DE LA RUTA MÁS CORTA

Empecemos nuestro estudio de los algoritmos de enrutamiento con una técnica simple para calcular las rutas óptimas con base en una imagen completa de la red. Estas rutas son las que queremos que encuentre un algoritmo de enrutamiento distribuido, aun cuando no todos los enrutadores conozcan todos los detalles de la red. La idea es construir un grafo de la red, en donde cada nodo del grafo representa un enrutador y cada arco del grafo representa una línea o enlace de comunicaciones. Para elegir una ruta entre un par específico de enrutadores, el algoritmo simplemente encuentra la ruta más corta entre ellos en el grafo. El concepto de la ruta más corta merece una explicación. Una manera de medir la longitud de una ruta es mediante el número de saltos. Con base en esta métrica, las rutas ABC y ABE en la figura son igual de largas. Otra métrica es la distancia geográfica en kilómetros, en cuyo caso ABC es sin duda mucho más larga que ABE (suponiendo que la figura esté dibujada a escala). Sin embargo, también son posibles muchas otras métricas además de los saltos y la distancia física. Por ejemplo, cada arco se podría etiquetar con el retardo promedio de un paquete de prueba estándar, determinado por una serie de pruebas cada hora. Con estas etiquetas en el grafo, la ruta más corta es la ruta más rápida, en lugar de la ruta con menos arcos o kilómetros.



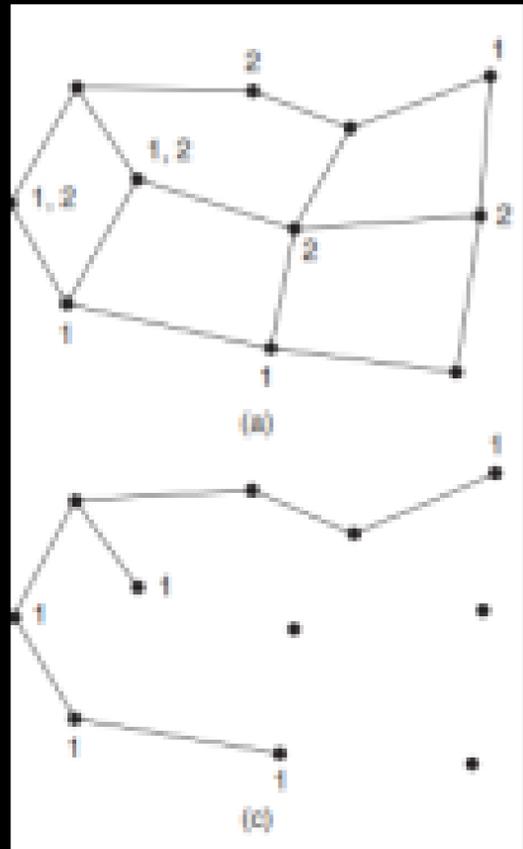
3.8. ENRUTAMIENTO POR DIFUSIÓN

En algunas aplicaciones, los hosts necesitan enviar mensajes a varios o a todos los hosts en la red. Por ejemplo, el servicio de distribución de informes sobre el clima, la actualización de los precios de la bolsa o los programas de radio en vivo podrían funcionar mejor si se difunden a todas las máquinas para dejar que las personas interesadas lean los datos. El envío simultáneo de un paquete a todos los destinos se llama difusión (broadcasting). Se han propuesto varios métodos para llevarla a cabo. Ya hemos visto una mejor técnica de enrutamiento por difusión: la inundación. Cuando se implementa con un número de secuencia por cada origen, la inundación usa los enlaces de manera eficiente con una regla de decisión en los enrutadores que es relativamente simple. Aunque la inundación es poco adecuada para la comunicación punto a punto ordinaria, para difusión puede merecer que se le considere con seriedad. La idea del reenvío por ruta invertida (reverse path forwarding) es elegante y excepcionalmente sencilla una vez planteada (Dalal y Metcalfe, 1978). Cuando llega un paquete difundido a un enrutador, éste lo revisa para ver si llegó por el enlace que se usa por lo común para enviar paquetes hacia el origen de la difusión. De ser así, hay excelentes posibilidades de que el paquete difundido haya seguido la mejor ruta desde el enrutador y, por lo tanto, sea la primera copia en llegar al enrutador. Si éste es el caso, el enrutador reenvía copias del paquete a todos los enlaces, excepto a aquel por el que llegó.



3.9. ENRUTAMIENTO MULTIDIFUSIÓN

Algunas aplicaciones, como un juego multijugador o un video en vivo de un evento deportivo que se transmite por flujo continuo a muchas ubicaciones, envían paquetes a múltiples receptores. A menos que el grupo sea muy pequeño, es costoso enviar un paquete distinto a cada receptor. Por otro lado, sería un desperdicio difundir un paquete si el grupo consiste en, por decir, 1000 máquinas en una red con un millón de nodos, de tal forma que la mayoría de los receptores no están interesados en el mensaje (o peor aún, están en definitiva interesados pero se supone que no deben verlo). Por lo tanto, necesitamos una manera de enviar mensajes a grupos bien definidos que sean grandes en número, pero pequeños en comparación con la totalidad de la red. El proceso de enviar un mensaje a uno de tales grupos se denomina multidifusión (multicasting); el algoritmo de enrutamiento que se utiliza es el enrutamiento por multidifusión. Todos los esquemas de multidifusión requieren alguna forma de crear y destruir grupos, además de identificar qué enrutadores son miembros de un grupo. La forma de realizar estas tareas no le concierne al algoritmo de enrutamiento. Por ahora vamos a suponer que cada grupo se identifica mediante una dirección de multidifusión y que los enrutadores conocen los grupos a los que pertenecen.



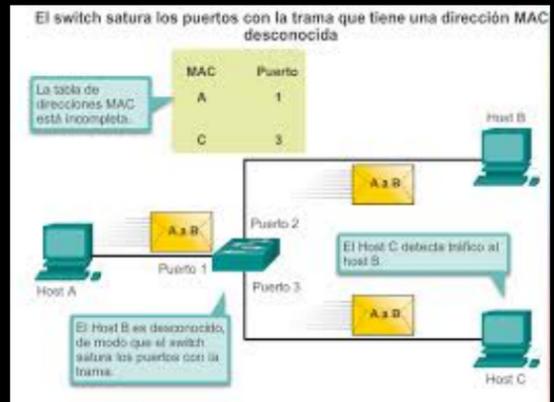
3.10. ELEMENTOS DE UN SWITCH

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. Como por ejemplo un PC, portátil, un router, otro switch, una impresora y en general cualquier dispositivo que incluya una interfaz de red Ethernet. El número de puertos es una de las características básicas de los switches. Aquí existe un abanico bastante amplio, desde los pequeños switches de 4 puertos hasta switches troncales que admiten varios cientos de puertos. El estándar Ethernet admite básicamente dos tipos de medios de transmisión cableados: el cable de par trenzado y el cable de fibra óptica. El conector utilizado para cada tipo lógicamente es diferente así que otro dato a tener en cuenta es de qué tipo son los puertos. Normalmente los switches básicos sólo disponen de puertos de cable de par trenzado (cuyo conector se conoce como RJ-45) y los más avanzados incluyen puertos de fibra óptica (el conector más frecuente aunque no el único es el de tipo SC)



3.11. PROCESO DE ARRANQUE DEL SWITCH.

Una vez que se enciende el switch Cisco, lleva a cabo la siguiente secuencia de arranque: 1. Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Esta comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash. 2. A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente. 3. El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad. 4. El cargador de arranque inicia el sistema de archivos flash en la placa del sistema. 5. Por último, el cargador de arranque ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al IOS.



3.12. CONCEPTOS

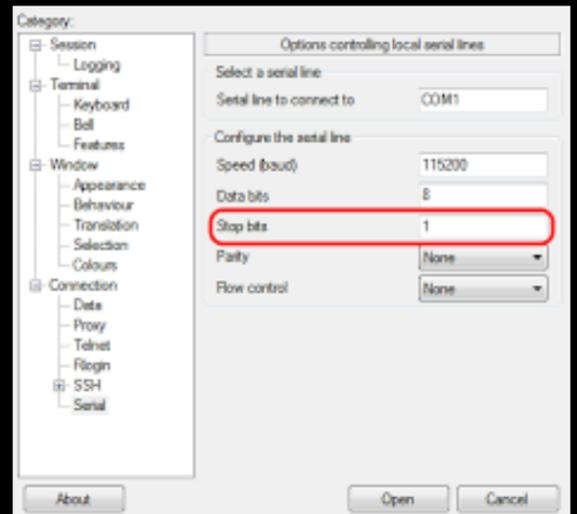
Post, (Power OnSelf Test): la rutina de autocomprobación que el sistema BIOS de un ordenador realiza al ser encendido. BIOS (siglas en inglés de Basic Input Output System, es decir, Sistema Básico de Entrada y Salida), RX, Receiver (o Receive) Data Datos del receptor (o recibidor) TX, Transmitter o Transmit Data Transmisor o transmitir datos CPU, (Siglas de central processing unit, unidad central de proceso) RAM: Random Access Memory(memoria de acceso aleatorio) ROM: Read Only Memory (Memoria de solo lectura) HD- disco duro (del inglés Hard Disk) IOS significa Sistema Operativo de Internet (Internet Operating System) BIOS (siglas en inglés de Basic Input Output System, es decir, Sistema Báístico de Entrada y salida). DCD (Data Carrier Detect) DTR (Data Terminal Ready) GND(ground) DSR (Data Sheet Ready) RTS (Request To Send) CTS (Clear To Send) RI (Ring Indicator) RX - Receiver (o Receive) Data , Datos del receptor (o recibidor). TX - (Transmitter o Transmit Data ,Transmisor o transmitir datos) TFTP (Trivial File Transfer Protocol)



3.13. INGRESO A LA CONSOLA DEL SWITCH.

Los routers Cisco y ciertos switches soportan la conectividad fuera de banda (sobre todo para la recuperación de catástrofes) mediante un módem que conecta con el puerto auxiliar o el puerto de consola. Los switches Cisco Catalyst no tienen puertos auxiliares. Por lo tanto, El módem conecta solamente con el puerto de consola. Tenga presente que la configuración de los puertos de la consola en los switches Catalyst está diseñada para un acceso fácil y rápido a través de cualquier dispositivo DTE RS-232 estándar (por ejemplo, un PC). Sin embargo, el diseño de los puertos de la consola no es para una accesibilidad remota con un DCE, como un módem. Este documento proporciona un procedimiento para marcar en el puerto de la consola de los switches de Catalyst. Nota: La conexión de los módems al puerto de la consola de un conmutador tiene algunas desventajas. Hay también problemas de seguridad cuyo ser consciente. Algunos ejemplos son los siguientes:

- El puerto de la consola no utiliza el control del módem RS232 (detección de la portadora DSR/Data [DCD], [DTR] listo del terminal de datos). Por lo tanto, cuando la sesión de EXEC termina (fin de comunicación), la conexión del módem no cae automáticamente; el usuario necesita desconectar manualmente la sesión.
- Más seriamente, si la conexión del módem cae, la sesión de EXEC no reajusta automáticamente. Este error reajustar presenta a una brecha en la seguridad; una llamada posterior en ese módem puede tener acceso a la consola sin la entrada de una contraseña. Usted puede hacer el agujero más pequeño si usted fija un tiempo de espera de EXEC corto en la línea. Sin embargo, en caso que la seguridad sea importante, utilice un módem que proporcione un mensaje de indicación de contraseña



3.14. ADMINISTRACIÓN DE LA TABLA DE DIRECCIONES MAC.

Manera en que los switches crean y administran las tablas de direcciones MAC Los switches examinan la dirección origen de las tramas que se reciben en los puertos para aprender la dirección MAC de las estaciones de trabajo o las PC conectadas a éstos. Estas direcciones MAC aprendidas se registran luego en una tabla de direcciones MAC. Las tramas que tienen una dirección MAC destino, que se ha registrado en la tabla, se pueden conmutar hacia la interfaz correcta. El comando `show mac-address-table` se puede introducir en el modo EXEC privilegiado para examinar las direcciones que un switch ha aprendido.

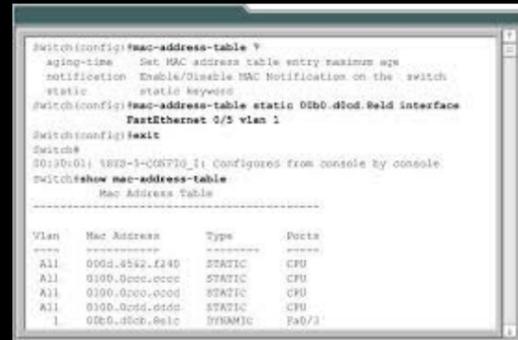
```
S1# show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
A11     0100.0ccc.cccc  STATIC CPU
A11     0100.0ccc.cccd  STATIC CPU
10      048c.b5ce.a8c0  DYNAMIC Fa0/4
10      000f.34f9.9201  DYNAMIC Fa0/5
10      5475.d08e.9ad8  DYNAMIC Fa0/13
Total Mac Addresses for this criterion: 5
```

La PC1 está conectada a Fa0/13 del S1, dentro de la VLAN 10.

Un switch aprende en forma dinámica y mantiene miles de direcciones MAC. Para preservar la memoria y para una operación óptima del switch, las entradas aprendidas se pueden descartar de la tabla de direcciones MAC. Es posible que se hayan eliminado máquinas de un puerto, se hayan apagado o trasladado a otro puerto en el mismo switch o en un switch diferente. Esto puede provocar confusión al momento de enviar las tramas. Por todas estas razones, si no se ven tramas con una dirección aprendida anteriormente, la entrada de direcciones MAC se descarta automáticamente o expiran después de 300 segundos.

3.15. CONFIGURACIÓN DE DIRECCIONES MAC

Al contrario de lo que puede parecer, una dirección MAC no sólo hace referencia a ordenadores de Mac. También de los de Microsoft. Se trata de un identificador de 48 bits (6 números hexadecimales) que está presente en todo dispositivo de red. Viene asignado por el fabricante. Un ejemplo de dirección MAC podría ser el siguiente: 00:1B:44:11:3A:B7. En este post vamos hablarte un poco de las direcciones MAC, cómo puedes identificar tus direcciones MAC en una red de dispositivos y qué es un filtro de direcciones MAC y cómo puedes hacer uno. Direcciones Mac ¿qué son? Son las siglas en inglés de Media Access Control, lo que traducido sería -control de acceso al medio|. Las direcciones MAC son únicas en todo el mundo. Se escriben en el hardware, de forma binaria, en el momento de llevarse a cabo la fabricación del dispositivo. Los primeros 24 bits (los tres primeros bloques hexadecimales) están configurados por el IEEE (Instituto de Ingeniería Eléctrica y Electrónica) y los otros 24 por el fabricante del dispositivo. Enrutadores, tarjetas de red, impresoras, tarjetas inalámbricas, tablets... todos los dispositivos tienen una dirección MAC, única e irrepetible. Generalmente no vas a necesitar conocer tu dirección MAC para las operaciones habituales, como configurar una conexión a Internet por cable, o crear una red doméstica de ordenadores.



REFERENCIAS

TODA LA INFORMACION DE ESTE TRABAJO SE TOMO DE LA ANTOLOGIA CORRESPONDIENTE A LA MATERIA DE REDES DE COMPUTADORAS II.